IN THE CLAIMS:

Claims 1, 15, 28, and 29 are amended herein. All pending claims and their present status are produced below.

1. (Currently Amended) A method of tracking a security state for an intermodal container through a global supply chain, comprising:

receiving credentials from a first trusted agent confirming the first trusted agent has trusted status;

initiating a security state for the intermodal container with information submitted by ~~a~~ the first trusted agent located at a first checkpoint;

continuously monitoring the security state of the container during transport between the first checkpoint and a second checkpoint, the security state adapted to change responsive a security breach;

receiving credentials from a second trusted agent confirming the second trusted agent has trusted status; and

sending the security state to ~~a~~ the second trusted agent located at the second checkpoint for validation.

2. (Original) The method of claim 1, wherein the step of initiating the security state comprises initiating the security state to a secure state responsive to an inspection by the first trusted agent.

3. (Original) The method of claim 1, wherein the step of continuously monitoring the security state comprises changing the security state responsive to a security breach defined by security business rules.

4. (Original) The method of claim 1, wherein the step of initiating the security state comprises initiating the security state with a required body of information comprising an expected transport route between the first checkpoint and the second checkpoint, and wherein the step of monitoring the security state comprises changing the security state if the actual transport route deviates from the expected transport route.

5. (Original) The method of claim 1, wherein the step of initiating the security state comprises initiating the security state with a required body of information comprising information related to authorized unsealing of the container, and wherein the monitoring the security state comprises changing the security state if the container is unsealed without authorization between the first checkpoint and the second checkpoint.

6. (Original) The method of claim 1, wherein the step of initiating the security state comprises initiating the security state with the required body of information comprising information concerning a unique identifier assigned to a seal that locks the container, and wherein the step of monitoring the security state comprises using the unique identifier to continually monitor the seal for a status.

7. (Original) The method of claim 6, wherein the status comprises one from the group consisting of: door open, attempt to open door, door closed, door locked, right door open, and more than one door open.

8. (Original) The method of claim 6, wherein the status comprises an environmental state from the group consisting of: temperature, humidity, vibration, shock, light, and radiation.

9. (Original) The method of claim 1, further comprising the steps of:

detecting the security breach; and

resetting the security state responsive to the second agent submitting an indication that the container was resecured.

10. (Original) The method of claim 1, further comprising the steps of:

receiving an inspection request from an authority; and

changing the security state responsive to the inspection request.

11. (Original) The method of claim 1, further comprising the steps of:

submitting a required body of information, including the information, to an authority;

wherein the authority sends the inspection request responsive to the required body of information.

12. (Original) The method of claim 1, wherein the first agent is located at an origin port of an export country and the second agent is located at a destination port of an import country.

13. (Original) The method of claim 1, wherein the step of monitoring comprises the steps of:

receiving monitor information from a first reader at the first checkpoint through a first control center;

receiving monitor information from a second reader on a transportation device; and

receiving monitor information from a third reader at the second checkpoint through a second control center.

14. (Original) The method of claim 1, wherein the container comprises an RFID (Radio Frequency IDentification) tag, and the first, second, and third readers each comprise an RFID reader.

15. (Currently Amended) A security state system for tracking a container through a global supply chain, comprising:

a first receiving module for receiving credentials from a first trusted agent confirming the first trusted agent has trusted status;

a required body of information module to store information concerning the container submitted by a first trusted agent located at a first checkpoint, the required body of information module coupled to the receiving module;

a second receiving module for receiving credentials from a second trusted agent confirming the second trusted agent has trusted status; and

a security state module, coupled to the information module and the second receiving module, the security state module initiating the security state based on the information, continuously monitoring the security state between the first checkpoint and a second checkpoint, the security state adapted to change responsive to a security breach, and the security state module sending the security state to a second trusted agent at the second checkpoint for validation.

16. (Original) The system of claim 15, wherein the security state module initiates the security state to a secure state responsive to an inspection by the first trusted agent.

17. (Original) The system of claim 15, wherein the security state module further comprises to change the security state responsive to a security breach defined by security business rules.

18. (Original) The system of claim 15, wherein the information comprises an expected transport route between the first checkpoint and the second checkpoint, and wherein the security state module changes the security state if the actual transport route deviates from the expected transport route.

19. (Original) The system of claim 15, wherein the information comprises authorized unsealing of the container, and wherein the security state module changes the security state if the container is unsealed without authorization between the first checkpoint and the second checkpoint.

20. (Original) The system of claim 15, wherein the information comprises a unique identifier assigned to a seal that locks the container, and wherein the security state module uses the unique identifier to continually monitor the seal for a status.

21. (Original) The system of claim 20, wherein the status comprises one from the group consisting of: door open, attempt to open door, door closed, door locked, right door open, and more than one door open.

22. (Original) The system of claim 20, wherein the status comprises an environmental state from the group consisting of: temperature, humidity, vibration, shock, light, and radiation.

23. (Original) The system of claim 15, further comprising a seal device to detect a security breach, wherein the security state module resets the security state responsive to the second agent submitting an indication that the container was resecured.

24. (Original) The system of claim 15, wherein the security state module changes the security state responsive to receiving an inspection request from a customs control center.

25. (Original) The system of claim 15, wherein the security state module submits a required body of information, including the information, to a customs control center, and receives an inspection request responsive to the required body of information.

26. (Original) The system of claim 15, wherein the first agent is located at an origin port of an export country and the second agent is located at a destination port of an import country.

27. (Original) The system of claim 15, wherein the required body of information module receives the information from a first reader at the first checkpoint through a first control center, the security state module receives continuous monitoring information from a second reader; and receives a validation confirmation from a third reader at the second checkpoint through a second control center.

28. (Currently Amended) The system of claim ~~15~~ 27, wherein the container comprises an RFID (radio frequency identification) tag, and the first, second, and third readers comprise an RFID reader.

29. (Currently Amended) A computer product~~, comprising:~~ having a computer-readable medium having computer program instructions ~~and data~~ embodied thereon ~~for~~ capable of causing a computer to perform a method of tracking a security state for an intermodal container through a global supply chain, the method comprising:

receiving credentials from a first trusted agent confirming the first trusted agent has trusted status;

initiating a security state for the intermodal container with information submitted by ~~a~~ the first trusted agent located at a first checkpoint;

continuously monitoring the security state of the container during transport between the first checkpoint and a second checkpoint, the security state adapted to change responsive a security breach;

receiving credentials from a second trusted agent confirming the second trusted agent has trusted status; and

sending the security state to ~~a~~ the second trusted agent located at the second checkpoint for validation.

30. (Original) The computer product of claim 29, wherein the step of initiating the security state comprises initiating the security state to a secure state responsive to an inspection by the first trusted agent.

31. (Original) The computer product of claim 29, wherein the step of continuously monitoring the security state comprises changing the security state responsive to a security breach defined by security business rules.

32. (Original) The computer product of claim 29, wherein the step of initiating the security state comprises initiating the security state with a required body of information comprising information concerning a unique identifier assigned to a seal that locks the container, and wherein the step of monitoring the security state comprises using the unique identifier to continually monitor the seal for a status.

33. (Original) The computer product of claim 29, further comprising the steps of:

detecting the security breach; and

resetting the security state responsive to the second agent submitting an indication that the container was resecured.

34. (Original) The computer product of claim 29, further comprising the steps of:

receiving an inspection request from an authority; and

changing the security state responsive to the inspection request.

35. (Original) The computer product of claim 29, further comprising the steps of:

submitting a required body of information, including the information, to an authority;

wherein the authority sends the inspection request responsive to the required body of information.

36. (Original) The computer product of claim 29, wherein the first agent is located at an origin port of an export country and the second agent is located at a destination port of an import country.